Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Protection Profile

Machine Readable Travel Document with „ICAO Application", Extended Access Control

BSI-PP-0026

Approved by the
Federal Ministry of the Interior

Version 1.1, 7th September 2006

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

Foreword

This ‘Protection Profile — Machine Readable Travel Document with ICAO Application (MRTD-PP), Extended Access Control’ is issued by Bundesamt für Sicherheit in der Informationstechnik, Germany.

The document has been prepared as a Protection Profile (PP) following the rules and formats of Common Criteria version 2.3 [1], [2], [3].

Correspondence and comments to this Machine Readable Travel Document (MRTD-PP) should be referred to:

CONTACT ADDRESS

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53175 Bonn, Germany

Tel +49 1888 9582-0
Fax +49 1888 9582-400

Email bsi@bsi.bund.de

Table of Content

1 PP Introduction

1.1 PP reference

1	Title:	Protection Profile — Machine Readable Travel Document with ICAO Application, Extended Access Control (PP-MRTD EAC)
	Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
	Editors:	Wolfgang Killmann, T-Systems GEI GmbH, Solution & Service Center Testfactory & Security
	CC Version:	2.3
	Assurance Level:	The minimum assurance level for this PP is EAL4 augmented.
	General Status:	Working draft
	Version Number:	1.1
	Registration:	BSI-PP-0026
	Keywords:	ICAO, machine readable travel document, extended access control

1.2 PP Overview

2 The protection profile defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control, Extended Access Control and chip authentication similar to the Active Authentication in the Technical reports of the ICAO New Technology Working Group.

1.3 Conformance Claim

3 This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-08-003

as follows

- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

2 TOE Description

TOE definition

4 The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [5] and providing the Basic Access Control, the Extended Access Control according to the ICAO document [6] and the chip authentication according to the technical report [25].

5 The TOE comprises of

- the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antennae, capacitors,
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application and
- the associated guidance documentation.

TOE usage and security features for operational use

6 State or organisation issues MRTD to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this protection profile contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

7 For this protection profile the MRTD is viewed as unit of

(a) the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder

(1) the biographical data on the biographical data page of the passport book,

(2) the printed data in the Machine Readable Zone (MRZ) and

(3) the printed portrait.

(b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [5] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder

(1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

(2) the digitized portraits (EF.DG2),

(3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1]

(4) the other data according to LDS (EF.DG5 to EF.DG16) and

[1] These biometric reference data are optional according to [5]. This PP assumes that the issuing State or Organization uses this option and protects these data by means of extended access control.

(5) the Document security object.

8 The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the document number.

9 The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organisational security measures (e.g. control of materials, personalization procedures) [7]. These security measures include the binding of the MRTD's chip to the passport book.

10 The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

11 The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Technical report [6]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

12 This protection profile addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism and the Extended Access Control Mechanism. This protection profile addresses the Chip Authentication described in [25] as an alternative to the Active Authentication stated in [6].

13 The Basic Access Control is a security feature that shall be mandatory implemented by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [6], Annex E, and [5].

14 The protection profile requires the TOE to implement the Chip Authentication defined in [25] instead of the Active Authentication described in [6]. Both protocols provide evidence of the MRTD's chip authenticity where the Chip Authentication prevents data traces described in [6], Annex G, section G.3.3. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates a ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. it could apply the Chip Authentication Private Key corresponding to the Chip Authentication Public Key for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

15 The protection profile requires the TOE to implement the Extended Access Control as defined in [25]. The Extended Access Control consists of two parts (i) a Terminal Authentication Protocol to authenticate the inspection system as entity authorized by the Issuing State or Organization through the receiving State, and (ii) an access control by the TOE to allow reading the sensitive

biometric reference data only to successfully authenticated authorized inspection systems. It requires the Chip Authentication of the MRTD's chip to the inspection system and uses the secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

TOE life cycle

16 The TOE life cycle is described in terms of the four life cycle phases.

Phase 1 "Development"

17 The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

18 The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

19 The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

Phase 2 "Manufacturing"

20 In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

21 The MRTD manufacturer (i) adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary, (ii) creates the MRTD application, (iii) equips MRTD's chips with pre-personalization Data, and (iv) combines the IC with hardware for the contactless interface in the passport book.

22 The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase 3 "Personalization of the MRTD"

23 The personalization of the MRTD includes (i) the survey of the MRTD holder's biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) the writing of the TSF Data into the logical MRTD and configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitised portrait (EF.DG2), and (iii) the Document security object.

24 The signing of the Document security object by the Document signer [6] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together

with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

25 **Application note 1:** This protection profile distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [6]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organisation, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralised personalization schemes but relies on stronger security protection in the personalization environment (cf. section 5.3.6 Personalization Terminals for further details).

Phase 4 "Operational Use"

26 The TOE is used as MRTD chip by the traveller and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the Issuing State or Organization and can be used according to the security policy of the Issuing State but they can never be modified.

27 **Application note 2:** The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 "Operational Use". This will imply an update of the Document Security Object including the re-signing by the Document Signer.

28 **Application note 3:** The intention of the PP is to consider at least the phases 1 and 2 as part of the evaluation and therefore to define the TOE delivery according to CC after phase 2 or later. The personalization process and its environment may depend on specific security needs of an issuing state or organisation. The Security Target shall describe the instantiation of the life cycle defined in this PP relevant for the product evaluation process. It is of importance to define the point of TOE delivery in the life cycle required for the evaluation according to CC requirements ADO_DEL. All development and production steps before TOE delivery have to be part of the evaluation under ACM, ALC and ADO assurance classes as specifically relevant before TOE delivery. All production, generation and installation procedures after TOE delivery up to the operational use (phase 4) have to be considered in the product evaluation process under ADO and AGD assurance classes. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery. Note: In many cases security aspects for phase 3 are defined and controlled by the issuing state or organisation.

3 Security Problem Definition

3.1 Introduction

Assets

29 The assets to be protected by the TOE include the User Data on the MRTD’s chip.

30 **Logical MRTD Data**
The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [5]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

User Data	TSF Data
Personal Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 - EF.DG13, EF.DG15, EF.DG16)	Personalisation Agent Reference Authentication Data
Sensitive biometric reference data (EF.DG3, EF.DG4)	Basic Access Control (BAC) Key
Chip Authentication Public Key in EF.DG14	Public Key CVCA
Document Security Object (SOD) in EF.SOD	CVCA Certificate
Common data in EF.COM	Current date
	Chip Authentication Private Key

31 A sensitive asset is the following more general one.

32 **Authenticity of the MRTD’s chip**
The authenticity of the MRTD’s chip personalized by the issuing State or Organization for the MRTD holder is used by the traveller to proof his possession of a genuine MRTD.

Subjects

33 This protection profile considers the following subjects:

34 **Manufacturer**
The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD’s chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

35 **Personalization Agent**
The agent is acting on behalf of the issuing State or Organisation to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national

interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [5].

36 **Country Verifying Certification Authority**
The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing Country or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in form of Country Verifying CA Link-Certificates.

37 **Document Verifier**
The Document Verifier (DV) enforces the privacy policy of the receiving Country with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in form of the Document Verifier Certificates.

38 **Terminal**
A terminal is any technical system communicating with the TOE through the contactless interface.

39 **Inspection system (IS)**
A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder. The **Basic Inspection System** (BIS) (i) contains a terminal for the contactless communication with the MRTD’s chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The **General Inspection System** (GIS) is a Basic Inspection System which implements additional the Chip Authentication Mechanism. The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

40 **Application note 4**: According to [6] the support of (i) the Passive Authentication mechanism is mandatory, and (ii) the Basic Access Control is optional. In the context of this protection profile the Primary Inspection System does not implement the terminal part of the Basic Access Control. It is therefore not able to read the logical MRTD because the logical MRTD of the TOE is protected by Basic Access Control. Therefore this protection profile will not consider the use of Primary Inspection System by the receiving State or Organization. The TOE of the current protection profile does not allow the Personalization agent to disable the Basic Access Control for use with Primary Inspection Systems as described in the BSI-PP-0017 Machine Readable Travel Document with „ICAO Application", Basic Access Control.

41 **MRTD Holder**
The rightful holder of the MRTD for whom the issuing State or Organization personalised the MRTD.

42 **Traveller**
Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

43 **Attacker**
A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

44 **Application note 5**: An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but his or her attack itself is not relevant for the TOE.

3.2 Assumptions

45 The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

46 **A.Pers_Agent** **Personalization of the MRTD's chip**

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

47 **A.Insp_Sys** **Inspection Systems for global interoperability**

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [6]. The Basic Inspection System reads the logical MRTD being under Basic Access Control and performs the Passive Authentication to verify the logical MRTD. The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

48 **A.Signature_PKI** **PKI for Passive Authentication**

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which (i) securely generates, stores and uses the Country Signing CA Key pair, and (ii) manages the MRTD's Chip Authentication Key Pairs. The CA keeps the Country Signing CA Private Key secret and distributes the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the

MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and organizations.

49 **A.Auth_PKI** **PKI for Inspection Systems**

The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the extended access control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organizations distributes the public key of their Country Verifying Certification Authority to their MRTD's chip.

3.3 Threats

50 This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in or protected by the TOE.

51 The TOE in collaboration with its IT environment shall avert the threats as specified below.

52 **T.Chip_ID** **Identification of MRTD's chip**

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless communication interface. The attacker cannot read optically and does not know in advance the physical MRTD.

53 **T.Skimming** **Skimming the logical MRTD**

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker cannot read and does not know in advance the physical MRTD.

54 **T.Read_Sensitive_Data** **Read the sensitive biometric reference data**

An attacker with high attack potential knowing the Document Basic Access Keys is trying to gain the sensitive biometric reference data through the communication interface of the MRTD's chip.

The attack T.Read_Sensitive_Data is similar to the threats T.Skimming in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visual readable on the physical MRTD as well.

55 **T.Forgery** **Forgery of data on MRTD's chip**

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose on an inspection system by means of the changed MRTD holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveller. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveller into an other MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD in another contactless chip.

56 **T.Counterfeit** **MRTD's chip**

An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveller by possession of a MRTD.

The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

57 The TOE shall avert the threat as specified below.

58 **T.Abuse-Func** **Abuse of Functionality**

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

59 **T.Information_Leakage** **Information Leakage from MRTD's chip**

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

60 Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA).

Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

61 **T.Phys-Tamper** **Physical Tampering**

An attacker may perform physical probing of the MRTD’s chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the MRTD’s chip Embedded Software. An attacker may physically modify the MRTD’s chip in order to (i) modify security features or functions of the MRTD’s chip, (ii) modify security functions of the MRTD’s chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data.

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD’s chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD’s chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

62 **T.Malfunction** **Malfunction due to Environmental Stress**

An attacker may cause a malfunction of TSF or of the MRTD’s chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD’s chip Embedded Software.

This may be achieved e.g. by operating the MRTD’s chip outside the normal operating conditions, exploiting errors in the MRTD’s chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

3.4 Organisational Security Policies

63 The TOE shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations (see CC part 1, sec. 3.2).

64 **P.Manufact** **Manufacturing of the MRTD’s chip**

The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD’s material in the Phase 2 Manufacturing. The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

65 **P.Personalization** **Personalization of the MRTD by issuing State or Organization only**

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitised portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorised by the issuing State or Organization only.

66 **P.Personal_Data** **Personal data protection policy**

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitised portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an inspection system. Additional to the Basic Access Control Authentication defined by ICAO in [6] the MRTD's chip shall protect the confidentiality and integrity of the personal data during transmission to the General Inspection System after Chip authentication.

67 **Application note 6:** The organisational security policy P.Personal_Data is drawn from the ICAO Technical Report [6]. Note, that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

68 **P.Sensitive_Data** **Privacy of sensitive biometric reference data**

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the MRTD holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the MRTD is presented to the inspection system. The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate.

3.5 Security Objectives

69 This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

3.5.1 Security Objectives for the TOE

70 This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organisational security policies to be met by the TOE.

71 **OT.AC_Pers** **Access Control for Personalization of logical MRTD**

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [5] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalisation. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

72 **Application note 7**:The OT.AC_Pers implies that

(1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization,

(2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordantly.

73 **OT.Data_Int** **Integrity of personal data**

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

74 **OT.Data_Conf** **Confidentiality of personal data**

The TOE must ensure the confidentiality of the data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 and the Document Security Object of the logical MRTD by granting read access to terminals successfully authenticated by as (i) Personalization Agent or (ii) Basic Inspection System or (iii) Extended Inspection System. The TOE implements the Basic Access Control as defined by ICAO [6] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

75 **Application note 8**:The traveller grants the authorization for reading the personal data in EF.DG1 to EF.DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication independent on the quality of the Document Basic Access Keys which is defined by the TOE environment and loaded into the TOE by the Personalization Agent. Any attack based on decision of the ICAO Technical Report [6] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective OT.Data_Conf.[2]

76 **OT.Sens_Data_Conf** **Confidentiality of sensitive biometric reference data**

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized inspection systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

77 **OT.Identification** **Identification and Authentication of the TOE**

The TOE must provide means to store IC Identification Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". In Phase 4 "Operational Use", the

[2] Cf. CEM [4], section 8.10.3.4, para. 1625

TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

78 **Application note 9:** The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 “Manufacturing” and for traceability and/or to secure shipment of the TOE from Phase 2 “Manufacturing” into the Phase 3 “Personalization of the MRTD”. The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing environment as described in its security objective OD.Material. In the Phase 4 “Operational Use” the TOE is identified by the passport number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit serial number ICCSN) or a MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

79 **OT.Chip_Auth_Proof Proof of MRTD’S chip authenticity**

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD’s chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [25]. The authenticity prove provided by MRTD’s chip shall be protected against attacks with high attack potential.

80 **Application note 10:** The OT.Chip_Auth_Proof implies the MRTD’s chip to have (i) a unique identity as given by the MRTD’s Document number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD’s chip i.e. a certificate for the Chip Authentication Public Key that fit to the Chip Authentication Private Key of the MRTD’s chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [5] and (ii) the hash value of the Authentication Public Key in the Document Security Object signed by the Document Signer.

81 The following TOE security objectives address the protection provided by the MRTD’s chip independent on the TOE environment.

82 **OT.Prot_Abuse-Func Protection against Abuse of Functionality**

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smartcard Embedded Software, (iii) to manipulate Soft-coded Smartcard Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

83 **OT.Prot_Inf_Leak Protection against Information Leakage**

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD’s chip

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and

- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

84 **Application note 11:** This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

85 **OT.Prot_Phys-Tamper Protection against Physical Tampering**

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with high attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

- reverse-engineering to understand the design and its properties and functions.

86 **Application note 12:** In order to meet the security objectives OT.Prot_Phys-Tamper the TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack. This is addressed by the security objective OD.Assurance.

87 **OT.Prot_Malfunction Protection against Malfunctions**

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

88 **Application note 13:** A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

3.5.2 Security Objectives for the Development and Manufacturing Environment

89 **OD.Assurance Assurance Security Measures in Development and Manufacturing Environment**

The developer and manufacturer ensure that the TOE is designed and fabricated such that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through attack. This includes the use of the Initialization Data for unique identification of the

TOE and the pre-personalization of the TOE including the writing of the Personalization Agent Authentication key(s). The developer provides necessary evaluation evidence that the TOE fulfils its security objectives and is resistant against obvious penetration attacks with high attack potential.

90 **OD.Material** **Control over MRTD Material**

The IC Manufacturer, the MRTD Manufacturer and the Personalization Agent must control all materials, equipment and information to produce, initialise, pre-personalize genuine MRTD's materials and to personalize authentic MRTDs in order to prevent counterfeit of MRTDs using MRTD materials.

3.5.3 Security Objectives for the Operational Environment

Issuing State or Organization

91 The Issuing State or Organization will implement the following security objectives of the TOE environment.

92 **OE.Personalization** **Personalization of logical MRTD**

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organisation (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enrol the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

93 **OE.Pass_Auth_Sign** **Authentication of logical MRTD by Signature**

The Issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and organizations maintaining its authenticity and integrity. The Issuing State or organization must (i) generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signing Public Key to receiving States and organizations. The digital signature in the Document Security Object relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [5].

94 **OE.Auth_Key_MRTD** **MRTD Authentication Key**

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

95 **OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data**

The issuing State or Organization has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of MRTD's holders to authorized receiving States or Organizations. The Country Verifying Certification Authority of the issuing State or Organization generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

Receiving State or organization

96 The Receiving State or Organization will implement the following security objectives of the TOE environment.

97 **OE.Exam_MRTD Examination of the MRTD passport book**

The inspection system of the Receiving State must examine the MRTD presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [6]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

98 **OE.Passive_Auth_Verif Verification by Passive Authentication**

The border control officer of the Receiving State uses the inspection system to verify the traveller as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and organizations must manage the Country Signing Public Key and the Document Signing Public Key maintaining their authenticity and availability in all inspection systems.

99 **OE.Prot_Logical_MRTD Protection of data of the logical MRTD**

The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical MRTD. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

100 **Application note 14**: The figure 2.1 in [25] supposes that the GIS and the EIS follow the order (i) running the Basic Access Control Protocol, (ii) reading and verifying only those parts of the logical MRTD after which are necessary to know for the Chip Authentication Mechanism (i.e. Document Security Object and Chip Authentication Public Key), (iii) running the Chip Authentication protocol, and (iv) reading and verifying the less-sensitive data of the logical MRTD after Chip Authentication. The supposed sequence has the advantage that the less-sensitive data are protected by secure messaging with cryptographic keys based on the Chip Authentication Protocol which quality is under control of the TOE. The inspection system will prevent additionally eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. Note that reading the less-sensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this PP. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

101 **OE.Ext_Insp_Systems Authorisation of Extended Inspection Systems**

The Document Verifier of receiving States or Organizations authorize Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical MRTD. The Extended Inspection System authenticates themselves to the MRTD's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

4 Extended Components Definition

102 This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [22], other components are defined in this protection profile.

4.1 Definition of the Family FAU_SAS

103 To define the security functional requirements of the TOE a sensitive family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

104 The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component levelling

FAU_SAS Audit data storage
1

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to store [assignment: *list of audit information*] in the audit records.

Dependencies: No dependencies.

4.2 Definition of the Family FCS_RND

105 To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component

FCS_RND is not limited to generation of cryptographic keys as the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.

106 The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component levelling:

FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

Dependencies: No dependencies.

4.3 Definition of the Family FIA_API

107 To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

108 **Application note 15**: The other families of the Class FIA describe only the authentication verification of users’ identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter “Explicitly stated IT security requirements (APE_SRE)”) form a TOE point of view.

109 **FIA_API Authentication Proof of Identity**

Family behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

FIA_API Authentication Proof of Identity
1

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or rule*].

Dependencies: No dependencies.

4.4 Definition of the Family FMT_LIM

110 The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

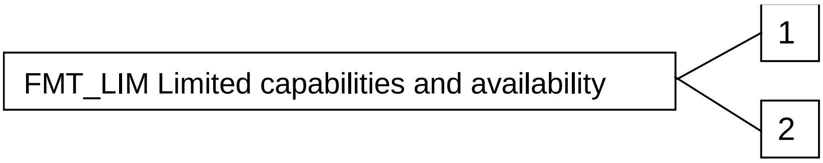
111 The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

112 To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

113 The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: *Limited capability and availability policy*].

Dependencies: FMT_LIM.2 Limited availability.

114 The TOE Functional Requirement "Limited availability (FMT_LIM.2)" is specified as follows.

FMT_LIM.2 **Limited availability**

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].

Dependencies: FMT_LIM.1 Limited capabilities.

115 **Application note 16:** The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

(ii) the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

The combination of both requirements shall enforce the policy.

4.5 Definition of the Family FPT_EMSEC

116 The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [2].

117 The family “TOE Emanation (FPT_EMSEC)” is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC TOE emanation
1

FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

Dependencies: No other components.

5 Security Requirements

118 The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this PP.

119 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "refinement" in bold text and the added/changed words are in **bold text**. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

120 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as unlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.

121 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*.

122 The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

123 The following table provides an overview of the keys and certificates used:

Name	Data
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [25] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security

Name	Data
	attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE’s logical MRTD and used by the inspection system for Chip Authentication of the MRTD’s chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic MRTD’s chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the Issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by Receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the Issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the Receiving State or organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD’s chip.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.

124 **Application note 17:** The Country Verifying Certification Authority identifies a Document Verifier as “domestic” in the Document Verifier Certificate if it belongs to the same country as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as “foreign” in the Document Verifier Certificate if it does belong to the same country as the Country Verifying Certification Authority. From MRTD’s point of view the domestic Document Verifier belongs to the issuing Country or Organisation.

5.1 Security Functional Requirements for the TOE

125 This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

5.1.1 Class FAU Security Audit

126 The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

127 **FAU_SAS.1 Audit storage**

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[3] with the capability to store the IC Identification Data [4] in the audit records.

Dependencies: No dependencies.

128 **Application note 18:** The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS). The security measures in the manufacturing environment assessed under ADO_IGS and ADO_DEL ensure that the audit records will be used to fulfil the security objective OD.Assurance.

5.1.2 Class Cryptographic Support (FCS)

129 The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

130 **FCS_CKM.1/KDF_MRTD Cryptographic key generation – Key Derivation Function by the MRTD**

Hierarchical to: No other components.

FCS_CKM.1.1/ KDF_MRTD The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm [5] and specified cryptographic key sizes 112 bit[6] that meet the following: [6], Annex E [7].

[3] [assignment: *authorised users*]

[4] [assignment: *list of audit information*]

[5] [*assignment: cryptographic key generation algorithm*]

[6] [*assignment: cryptographic key sizes*]

[7] [assignment: *list of standards*]

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

131 **Application note 19:** The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [6], Annex E.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC BAC Session Keys for secure messaging by the algorithm in [6], Annex E.1. The TOE uses this key derivation function to derive other session keys from shared secrets established by the Chip Authentication Protocol for the secure messaging required by FCS_COP.1/ENC_MRTD and FCS_COP.1/MAC_MRTD as well. The TOE may use this key derivation function for authentication of the Personalization Agent. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1/MRTD.

132 **FCS_CKM.1/DH_MRTD Cryptographic key generation – Diffie-Hellman Keys by the MRTD**

Hierarchical to: No other components.

FCS_CKM.1.1/ DH_MRTD The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [25], Annex A.1 [8].

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

133 **Application note 20:** The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [25], sec. 3.1 and Annex A.1. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. a modulo arithmetic based cryptographic algorithm, cf. [21]) or on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [25], Annex A.1, [26] and [20] for details). The shared secret value is used to derive the 112 bit Triple-DES key for encryption and the 112 bit Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [6], annex E.1, for the TSF required by FCS_COP.1/ENC_MRTD and FCS_COP.1/MAC_MRTD.

134 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2).

135 **FCS_CKM.4 Cryptographic key destruction - MRTD**

Hierarchical to: No other components.

FCS_CKM.4.1/ The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key*

[8] [assignment: *list of standards*]

MRTD *destruction method*] that meets the following: [*assignment: list of standards*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

136 **Application note 21:** The TOE shall destroy the BAC Session Keys (i) after detection of an error in a received command by verification of the MAC, and (ii) after successful run of the Chip Authentication Protocol. The TOE shall destroy the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new power-on-session.

5.1.2.1 Cryptographic operation (FCS_COP.1)

137 The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

138 **FCS_COP.1/SHA_MRTD Cryptographic operation – Hash for Key Derivation by MRTD**

Hierarchical to: No other components.

FCS_COP.1.1/ SHA_MRTD The TSF shall perform hashing [9] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes none [10] that meet the following: FIPS 180-2 [11].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

139 **Application note 22:** The ST writer shall perform the missing operation for the assignment of the hash algorithm supported by the TOE. The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism (cf. [6], annex E.1). The Chip Authentication Protocol may use SHA-1 (cf. [25], Annex A.1.1). The TOE may implement additional hash functions SHA-224, and SHA-256 for the Terminal Authentication Protocol (cf. [25], Annex A.2.2 for details).

140 **FCS_COP.1/TDES_MRTD Cryptographic operation – Encryption / Decryption Triple DES**

Hierarchical to: No other components.

[9] [assignment: *list of cryptographic operations*]

[10] [assignment: *cryptographic key sizes*]

[11] [assignment: *list of standards*]

FCS_COP.1.1/ TDES_MRTD	The TSF shall perform secure messaging – encryption and decryption [12] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode [13] and cryptographic key sizes 112 bit [14] that meet the following: FIPS 46-3 [13] and [6]; Annex E.3 [15].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

141 **Application note 23:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of (i) the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/KDF_MRTD or (ii) the Chip Authentication Protocol according to the FCS_CKM.1/DH_MRTD. Note the Triple-DES in CBC mode with zero initial vector include also the Triple-DES in ECB mode for blocks of 8 byte used to check the authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism.

142 **FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC**

Hierarchical to: No other components.

FCS_COP.1.1/ MAC_MRTD	The TSF shall perform secure messaging – message authentication code [16] in accordance with a specified cryptographic algorithm Retail MAC [17] and cryptographic key sizes 112 bit [18] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [19].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

143 **Application note 24:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism as part of (i) the Basic Access Control Authentication Mechanism according to the

[12] [assignment: *list of cryptographic operations*]

[13] [assignment: *cryptographic algorithm*]

[14] [assignment: *cryptographic key sizes*]

[15] [assignment: *list of standards*]

[16] [assignment: *list of cryptographic operations*]

[17] [assignment: *cryptographic algorithm*]

[18] [assignment: *cryptographic key sizes*]

[19] [assignment: *list of standards*]

FCS_CKM.1/KDF_MRTD or (ii) the Chip Authentication Protocol according to the FCS_CKM.1/DH_MRTD.

144 **FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by MRTD**

Hierarchical to: No other components.

FCS_COP.1.1/ SIG_VER The TSF shall perform digital signature verification [20] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

145 **Application note 25:** The ST writer shall perform the missing operation of the assignments for the signature algorithms key lengths and standards implemented by the TOE for the Terminal Authentication Protocol (cf. [25], Annex A.2.1.1 and C.3 for details). The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

5.1.2.2 Random Number Generation (FCS_RND.1)

146 The TOE shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below (Common Criteria Part 2 extended).

147 **FCS_RND.1/MRTD Quality metric for random numbers**

Hierarchical to: No other components.

FCS_RND.1.1/ MRTD The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

Dependencies: No dependencies.

148 **Application note 26:** This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4/MRTD.

5.1.3 Class FIA Identification and Authentication

149 **Application note 27:** The Table 1 provides an overview on the authentication mechanisms used.

[20] [assignment: *list of cryptographic operations*]

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [6], Annex E, and [25]
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys
Basic Access Control Authentication Mechanism	FIA_AFL.1, FIA_UAU.4/MRTD, FIA_UAU.6/MRTD	FIA_UAU.4/BT, FIA_UAU.6/BT	Triple-DES, 112 bit keys and Retail-MAC, 112 bit keys
Chip Authentication Protocol	FIA_API.1/MRTD, FIA_UAU.5/MRTD, FIA_UAU.6/MRTD	FIA_UAU.4/GIS, FIA_UAU.5/GIS, FIA_UAU.6/GIS	DH or ECDH and Retail-MAC, 112 bit keys
Terminal Authentication Protocol	FIA_UAU.5/MRTD	FIA_API.1/EIS	RSASSA-PKCS1-v1_5 or EC-DSA with SHA

Table 1: Overview on authentication SFR

Note the Chip Authentication Protocol include the asymmetric key agreement and the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

150 The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2).

151 **FIA_UID.1 Timing of identification**

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow

(1) to establish the communication channel,
(2) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[21]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

152 **Application note 28:** The MRTD's chip and the terminal establish the communication channel through the contactless. The Protocol Type A defines an "Answer to Select" (ATS) and the protocol Type B is managed through the commands "Answer to Request" and "Answer to Attrib". Note that the terminal and the MRTD's chip use an identifier for the communication channel to allow the terminal for communication with more then one RFID. If the historical bytes are used to identify the product as usual for example with hard-mask version and component code (specific to the manufacturer), in particular context this could lead to an exploitation of the threat

[21] [assignment: *list of TSF-mediated actions*]

T.Chip_Id (e.g. in the case a MRTD holder has a chip manufactured by a local manufacturer, he could be traced in a foreign country where few holders could have the same ATS content). Therefore the ATS has to be set in such a manner, that it will not lead to a vulnerability by the means of identifying the chip (e.g. randomly using random number generator as required by FCS_RND.1).

153 **Application note 29:** In the "Operation Use" phase the MRTD must not allow anybody to read the ICCSN or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note, that the terminal and the MRTD's chip use an identifier for the communication channel to allow the terminal for communication with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

154 **Application note 30:** In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System. After successful authentication as Basic Inspection System the terminal may identify themselves as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or (ii) if necessary and available as Personalization Agent by selection of the Personalization Agent Authentication Key.

155 The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2).

156 **FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow

1. to establish the communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
3. to identify themselves by selection of the authentication key [22]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification.

[22] [assignment: *list of TSF-mediated actions*]

157 The TOE shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (Common Criteria Part 2).

158 **FIA_UAU.4/MRTD Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**

Hierarchical to: No other components.

FIA_UAU.4.1/ MRTD	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism, 2. Terminal Authentication Protocol, 3. Authentication Mechanism based on Triple-DES [23].

Dependencies: No dependencies.

159 **Application note 31:** All listed authentication mechanisms uses a challenge of 8 Bytes freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt: The Basic Access Control Authentication Mechanism, the Terminal Authentication Protocol and the Authentication Mechanism based on Triple-DES use RND.ICC [25].

160 **Application note 32:** The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [6]. In the first step the terminal authenticates itself to the MRTD’s chip and the MRTD’s chip authenticates to the terminal in the second step. In the first step the TOE sends a randomly chosen challenge which shall contain sufficient entropy to prevent T.Chip_ID. In the second step the MRTD’s chip provides a challenge-response-pair which allows the terminal a unique identification of the MRTD’s chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop the communication with the terminal not successfully authenticated in the first step of the protocol to fulfil the security objective OT.Identification and to prevent T.Chip_ID.

161 The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below (Common Criteria Part 2).

162 **FIA_UAU.5/MRTD Multiple authentication mechanisms**

Hierarchical to: No other components.

FIA_UAU.5.1/ MRTD	The TSF shall provide 1. Basic Access Control Authentication Mechanism, 2. Terminal Authentication Protocol, 3. Secure messaging in MAC-ENC mode, 4. Symmetric Authentication Mechanism based on Triple-DES [24] to support user authentication.

[23] [assignment: *identified authentication mechanism(*s)]

[24] [assignment: *list of multiple authentication mechanisms*]

FIA_UAU.5.2/ MRTD The TSF shall authenticate any user’s claimed identity according to the following rules:

1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms
   (a) the Basic Access Control Authentication Mechanism with Personalization Agent Keys,
   (b) the Symmetric Authentication Mechanism with Personalization Agent Key,
   (c) the Terminal Authentication Protocol with Personalization Agent Keys.
2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
3. After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of secure messaging with the key agreed upon with the authenticated terminal by means of the Basic Access Control Authentication Mechanism.
4. After run of the Chip Authentication Mechanism the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.
5. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism.[25].

Dependencies: No dependencies.

163 **Application note 33:** Depending on the authentication methods used the Personalization Agent holds (i) a pair of a Triple-DES encryption key and a retail-MAC key for the Basic Access Control Mechanism specified in [6], or (ii) a Triple-DES key for the Symmetric Authentication Mechanism or (iii) an asymmetric key pair for the Terminal Authentication Protocol (e.g. provided by the Extended Access Control PKI in a valid card verifiable certificate with appropriate encoded access rights). The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the secure messaging after the mutual authentication. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.

[25] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

164 The TOE shall meet the requirement “Re-authenticating (FIA_UAU.6)” as specified below (Common Criteria Part 2).

165 **FIA_UAU.6/MRTD Re-authenticating – Re-authenticating of Terminal by the TOE**

Hierarchical to: No other components.

FIA_UAU.6.1/ MRTD The TSF shall re-authenticate the user under the conditions

1. Each command sent to the TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall be verified as being sent by the authenticated BIS.
2. Each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS. [26]

Dependencies: No dependencies.

166 **Application note 34:** The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [6] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC_MRTD for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accept only those commands received from the initially authenticated user.

167 **Authentication failure handling (FIA_AFL.1)**

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

Dependencies: FIA_UAU.1 Timing of authentication

168 **Application note 35:** The ST writer shall perform the open operation in the elements FIA_AFL.1.1 and FIA_AFL.1.2. These assignments should be assigned to ensure especially the high strength of authentication function as terminal part of the Basic Access Control Authentication Protocol or (if necessary) of the Extended Access Control Authentication Protocol.
The ST writer may consider the following example for such operations and refinement:
FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 10 **consecutive** unsuccessful authentication attempts occur related to BAC authentication protocol.
FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or

[26] [assignment: *list of conditions under which re-authentication is required*]

surpassed, the TSF shall wait for an administrator configurable time between the receiving the terminal challenge e_{IFD} and sending the TSF response e_{ICC} during the BAC authentication attempts.
The terminal challenge e_{IFD} and the TSF response e_{ICC} are described in [25], Appendix C. The refinement by inclusion of the word "consecutive" allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the "consecutive unsuccessful authentication attempts" are count independent on power-on sessions but reset to zero after successful authentication only.

169 The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended).

170 **FIA_API.1/CAP Authentication Proof of Identity - MRTD**

Hierarchical to: No other components.

FIA_API.1.1/CAP The TSF shall provide a Chip Authentication Protocol according to [25] [27] to prove the identity of the TOE [28].

Dependencies: No dependencies.

171 **Application note 36:** This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [25]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [6], Annex E.1. The terminal verifies by means of secure messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

5.1.4 Class FDP User Data Protection

172 The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2).

173 **FDP_ACC.1 Subset access control**

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the Access Control SFP [29] on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD [30].

[27] [assignment: *authentication mechanism*]

[28] [assignment: *authorized user or rule*]

[29] [assignment: *access control SFP*]

[30] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Dependencies: FDP_ACF.1 Security attribute based access control

174 **Application note 37:** The Basic Access Control SFP addresses the configuration of the TOE for usage with Basic Inspection Systems only.

175 The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below (Common Criteria Part 2).

176 **FDP_ACF.1 Security attribute based access control**

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the Access Control SFP[31] to objects based on the following:

1. Subjects:
   - a. Personalization Agent,
   - b. Basic Inspection System,
   - c. Extended Inspection System
   - d. Terminal,
2. Objects:
   - a. data EF.DG1 to EF.DG16 of the logical MRTD,
   - b. data in EF.COM,
   - c. data in EF.SOD,
3. Security attributes:
   - a. authentication status of terminals,
   - b. Terminal Authorization [32].

[31] [assignment: *access control SFP*]

[32] [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
3. the successfully authenticated Extended Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
4. the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG3 according to the Terminal Authorization,
5. the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG4 according to the Terminal Authorization [33].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following sensitive rules: none[34].

FDP_ACF.1.4

1. The TSF shall explicitly deny access of subjects to objects based on the rule: A terminal authenticated as CVCA is not allowed to read to read data in the EF.DG3,
2. A terminal authenticated as CVCA is not allowed to read to read data in the EF.DG4,
3. A terminal authenticated as DV is not allowed to read to read data in the EF.DG3,
4. A terminal authenticated as DV is not allowed to read to read data in the EF.DG4,
5. the Terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD [35].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

177 **Application note 38:** The TOE verifies the certificate chain established by the Country Verifier Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifier Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

178 The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

[33] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[34] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

[35] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

179 **FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD**

Hierarchical to: No other components.

FDP_UCT.1.1/ MRTD The TSF shall enforce the Access Control SFP[36] to be able to transmit and receive[37] objects in a manner protected from unauthorised disclosure **after Chip Authentication**.

Dependencies: FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

180 The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2).

181 **FDP_UIT.1/MRTD Data exchange integrity - MRTD**

Hierarchical to: No other components.

FDP_UIT.1.1/ MRTD The TSF shall enforce the Access Control SFP [38] to be able to transmit and receive [39] user data in a manner protected from modification, deletion, insertion and replay [40] errors **after Chip Authentication**.

FDP_UIT.1.2/ MRTD The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [41] has occurred **after Chip Authentication**.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

182 **Application note 39:** FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication to the General Inspection System. The authentication mechanism as part of Basic Access Control Mechanism and the Chip Authentication Protocol establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

5.1.5 Class FMT Security Management

183 **Application note 40**: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

[36] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[37] [selection*: transmit, receive*]

[38] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[39] [selection*: transmit, receive*]

[40] [selection: *modification, deletion, insertion, replay*]

[41] [selection: *modification, deletion, insertion, replay*]

184 The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2).

185 **FMT_SMF.1 Specification of Management Functions**

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

1. Initialization,
2. Personalization,
3. Configuration [42].

Dependencies: No Dependencies

186 The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (Common Criteria Part 2).

187 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Country Verifier Certification Authority,
4. Document Verifier,
5. Basic Inspection System,
6. domestic Extended Inspection System
7. foreign Extended Inspection System [43].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Hierarchical to: FIA_UID.1 Timing of identification.

188 **Application note 41**: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

189 The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

190 **FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

[42] [assignment: *list of security management functions to be provided by the TSF*]

[43] [assignment: *the authorised identified roles*]

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow,

1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks [44]

Dependencies: FMT_LIM.2 Limited availability.

191 The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

192 **FMT_LIM.2 Limited availability**

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow

1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks [45].

Dependencies: FMT_LIM.1 Limited capabilities.

193 **Application note 42:** The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

194 The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

195 **FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data**

[44] [assignment: *Limited capability and availability policy*]

[45] [assignment: *Limited capability and availability policy*]

Hierarchical to: No other components.

FMT_MTD.1.1/ INI_ENA The TSF shall restrict the ability to write [46] the Initialization Data and Pre-personalization Data [47] to the Manufacturer [48].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

196 **Application note 43:** The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Authentication Key.

197 **FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data**

Hierarchical to: No other components.

FMT_MTD.1.1/ INI_DIS The TSF shall restrict the ability to disable read access for users to [49] the Initialization Data [50] to the Personalization Agent [51].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

198 **Application note 44:** According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides an unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

199 **FMT_MTD.1/CVCA_INI Management of TSF data – Initialisation of CVCA Certificate and Current Date**

Hierarchical to: No other components.

[46] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[47] [assignment: *list of TSF data*]

[48] [assignment: *the authorised identified roles*]

[49] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[50] [assignment: *list of TSF data*]

[51] [assignment: *the authorised identified roles*]

FMT_MTD.1.1/
CVCA_INI

The TSF shall restrict the ability to write [52] the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifier Certification Authority Certificate,
3. initial Current Date [53]

to [assignment: *the authorised identified roles*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

200 **Application note 45:** The ST writer shall perform the missing operation in the component FMT_MTD.1.1/INI_CVCA. The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalisation phase or by the Personalization Agent (cf. [25], sec. 2.2.6). The initial Country Verifying Certification Authority Public Key (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifier Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

201 **FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifier Certification Authority**

Hierarchical to: No other components.

FMT_MTD.1.1/
CVCA_UPD

The TSF shall restrict the ability to update [54] the

1. Country Verifier Certification Authority Public Key,
2. Country Verifier Certification Authority Certificate [55]

to Country Verifier Certification Authority [56].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

202 **Application note 46:** The Country Verifier Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifier CA Link-Certificates (cf. [25], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifier CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [25], sec. 2.2.3 and 2.2.4).

203 **FMT_MTD.1/DATE Management of TSF data – Current date**

Hierarchical to: No other components.

[52] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[53] [assignment: *list of TSF data*]

[54] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[55] [assignment: *list of TSF data*]

[56] [assignment: *the authorised identified roles*]

FMT_MTD.1.1/ DATE

The TSF shall restrict the ability to modify [57] the Current date [58] to

1. Country Verifier Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System [59].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

204 **Application note 47**: The authorized roles are identified in identified in their certificate (cf. [25], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [25], annex A.3.3, for details).

205 **FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write**

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_WRITE

The TSF shall restrict the ability to write [60] the Document Basic Access Keys [61] to the Personalization Agent [62].

Dependencies: ADV_SPM.1 Informal TOE security policy model
FMT_MTD.1 Management of TSF data

206 **Application note 48:** The Country Verifying Certification Authority Public Key is the TSF data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.

207 **FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key**

Hierarchical to: No other components.

FMT_MTD.1.1/ CAPK

The TSF shall restrict the ability to [selection: *create, load*] [63] the Chip Authentication Private Key [64] to [assignment: *the authorised identified roles*].

[57] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[58] [assignment: *list of TSF data*]

[59] [assignment: *the authorised identified roles*]

[60] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[61] [assignment: *list of TSF data*]

[62] [assignment: *the authorised identified roles*]

[63] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[64] [assignment: *list of TSF data*]

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

208 **Application note 49:** The component FMT_MTD.1/CAPK is refined by (i) selecting other operations and (ii) defining a selection for the operations “create” and “load” to be performed by the ST writer. The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb “create” means here that the Chip Authentication Private Key is generated by the TOE itself. In the later case the ST writer shall include an appropriate instantiation of the component FCS_CKM.1 as SFR for this key generation. The ST writer shall perform the assignment for the authorised identified roles in the SFR component FMT_MTD.1/CAPK.

209 **FMT_MTD.1/KEY_READ Management of TSF data – Key Read**

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_READ The TSF shall restrict the ability to read [65] the

1. Document Basic Access Keys,
2. Chip Authentication Private Key,
3. Personalization Agent Keys [66]

to none [67].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

210 **FMT_MTD.3 Secure TSF data**

Hierarchical to: No other components.

FMT_MTD.3.1 The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data **of the Terminal Authentication Protocol and the Access Control**.

Dependencies: ADV_SPM.1 Informal TOE security policy model
FMT_MTD.1 Management of TSF data

Refinement: The certificate chain is valid if and only if

(1) the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,

(2) the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification

[65] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[66] [assignment: *list of TSF data*]

[67] [assignment: *the authorised identified roles*]

Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

(3) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

211 **Application note 50:** The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4 and FIA_UAU.5. The Terminal Authorisation is used as TSF data for access control required by FDP_ACF.1.

5.1.6 Class FPT Protection of the Security Functions

212 The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other. The SFR “Non-bypassability of the TSP (FPT_RVM.1)” and “TSF domain separation (FPT_SEP.1)” together with “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

213 The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified below (Common Criteria Part 2 extended):

214 **FPT_EMSEC.1 TOE Emanation**

Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [*assignment: types of emissions*] in excess of [assignment: *specified limits*] enabling access to Personalization Agent Authentication Key and Chip Authentication Private Key [68] and [assignment: *list of types of user data*].

[68] [assignment: *list of types of TSF data*]

FPT_EMSEC.1.2 The TSF shall ensure <u>any users</u> [69] are unable to use the following interface <u>smart card circuit contacts</u> [70] to gain access to <u>Personalization Agent Authentication Key and Chip Authentication Private Key</u> [71] and [assignment: *list of types of user data*].

Dependencies: No other components.

215 **Application note 51**: The ST writer shall perform the operation in FPT_EMSEC.1.1 and FPT_EMSEC.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

216 The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

217 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2).

218 **FPT_FLS.1 Failure with preservation of secure state**

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

(1) <u>Exposure to operating conditions where therefore a malfunction could occur,</u>

(2) <u>failure detected by TSF according to FPT_TST.1</u> **[72]**.

Dependencies: ADV_SPM.1 Informal TOE security policy model

219 The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2).

220 **FPT_TST.1 TSF testing**

Hierarchical to: No other components.

[69] [assignment: *type of users*]

[70] [assignment: *type of connection*]

[71] [assignment: *list of types of TSF data*]

[72] [assignment: *list of types of failures in the TSF*]

FPT_TST.1.1 The TSF shall run a suite of self tests [*selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*][*assignment: conditions under which self test should occur*] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Dependencies: FPT_AMT.1 Abstract machine testing.

221 **Application note 52**: The ST writer shall perform the operation in FPR_TST.1.1. If the MRTD's chip uses state of the art smart card technology it will run the some self tests at the request of the authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the "authorised user" Manufacturer in the Phase 2 "Manufacturing". Other self tests may run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 Operational Use, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operation claimed by the concrete product under evaluation.

222 The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

223 **FPT_PHP.3 Resistance to physical attack**

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing [73] to the TSF [74] by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

224 **Application note 53**: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

225 The following security functional requirements protect the TSF against bypassing and support the separation of TOE parts.

[73] [assignment: *physical tampering scenarios*]

[74] [assignment: *list of TSF devices/elements*]

226 The TOE shall meet the requirement “Non-bypassability of the TSP (FPT_RVM.1)” as specified below (Common Criteria Part 2).

227 **FPT_RVM.1 Non-bypassability of the TSP**

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

228 The TOE shall meet the requirement “TSF domain separation (FPT_SEP.1)” as specified below (Common Criteria Part 2).

229 **FPT_SEP.1 TSF domain separation**

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC

Dependencies: No dependencies.

230 **Application note 54**: The parts of the TOE which support the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” should be protected from interference of the other security enforcing parts of the MRTD’s chip Embedded Software.

5.2 Security Assurance Requirements for the TOE

231 The for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

232 The minimum strength of function is SOF-high.

233 **Application note 55:** The high minimum strength of function covers but is not limited to the TSF required by the SFR FIA_UAU.4, FCS_RND.1 and FPT_FLS.1 as far as probabilistic or permutational mechanisms are involved, e.g. due to challenges generated by the TOE and sent to the terminal or probabilistic self tests.

234 This protection profile does not contain any security functional requirement for which an explicit stated strength of function claim is required.

5.3 Security Requirements for the IT environment

235 This section describes the security functional requirements for the IT environment using the CC part 2 components.

236 Due to CCIMB Final Interpretation #58 these components are editorial changed to express the security requirements for the components in the IT environment where the original components are directed for TOE security functions. The editorial changes are indicated in **bold**.

5.3.1 Passive Authentication

237 The ICAO, the Issuing States or Organizations and the Receiving States or Organization run a public key infrastructure for the Passive Authentication. This public key infrastructure distributes and protects the Country Signing CA Keys and the Document Signing Keys to support the signing of the User Data (EF.DG1 to EF.DG16) by means of the Document Security Object. The Technical Report [6] describes the requirements to the public key infrastructure for the Passive Authentication.

238 The Document Signer of the Issuing State or Organization shall meet the requirement "Basic data authentication (FDP_DAU.1)" as specified below (Common Criteria Part 2).

239 **FDP_DAU.1/DS Basic data authentication – Passive Authentication**

Hierarchical to: No other components.

FDP_DAU.1.1/ DS	The **Document Signer** shall provide a capability to generate evidence that can be used as a guarantee of the validity of logical the MRTD (EF.DG1 to EF.DG16) and the Document Security Object[75].
FDP_DAU.1.2/ DS	The **Document Signer** shall provide Inspection Systems of Receiving States or Organization [76] with the ability to verify evidence of the validity of the indicated information.

Dependencies: No dependencies

5.3.2 Extended Access Control PKI

240 The CVCA and the DV shall establish a Document Verification PKI by generating asymmetric key pairs and certificates for the CVCA, DV and IS which may be verified by the TOE. The following SFR use the term "PKI" as synonym for entities like CVCA, DV and IS which may be responsible to perform the identified functionality.

[75] [assignment: *list of objects or information types*]

[76] [assignment: *list of subjects*]

241 **FCS_CKM.1/PKI Cryptographic key generation – Document Verification PKI Keys**

Hierarchical to: No other components.

FCS_CKM.1.1/PKI The **PKI** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [25], Annex A [77].

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

242 **FCS_COP.1/CERT_SIGN Cryptographic operation – Certificate Signing**

Hierarchical to: No other components.

FCS_COP.1.1/ CERT_SIGN The **PKI** shall perform <u>digital signature creation</u> [78] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

243 **Application note 56:** The ST writer shall perform the missing operation of the assignments for the signature algorithms key lengths and standards to be used by CVCA and DV to create certificates which may be verified by FCS_COP.1/SIG_VER implemented by the TOE for the Terminal Authentication Protocol (cf. [25], Annex A.2.1.1 and C.3 for details).

5.3.3 Basic Terminal

244 This section describes common security functional requirements to the Basic Inspection Systems and the Personalization Agent if it uses the Basic Access Control Mechanism with the Personalization Agent Authentication Keys. Both are called “Basic Terminals” (BT) in this section.

245 The Basic Terminal shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (Common Criteria Part 2).

[77] [assignment: *list of standards*]

[78] [assignment: *list of cryptographic operations*]

246 **FCS_CKM.1/KDF_BT Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal**

Hierarchical to: No other components.

FCS_CKM.1.1/KDF_BT The **Basic Terminal** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm [79] and specified cryptographic key sizes 112 bit [80] that meet the following: [assignment: *list of standards*].

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

247 **Application note 57:** The ST writer shall perform the open operation in the element FCS_CKM.1.1/KDF_BT. The assigned standard shall ensure that the Basic Inspection Terminal derives the same Document Basic Access Key as loaded by the Personalization Agent into the TOE and used by the TOE for FIA_UAU.4/BAC_MRTD. The [6], Annex E.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

248 The Basic Terminal shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (Common Criteria Part 2).

249 **FCS_CKM.4/BT Cryptographic key destruction - BT**

Hierarchical to: No other components.

FCS_CKM.4.1/BT The **Basic Terminal** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

250 **Application note 58:** The ST writer shall perform the operation in FCS_CKM.4.1/BT. The basic terminal shall destroy the Document Basic Access Keys of the MRTD and the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging after inspection of the MRTD.

[79] [*assignment: cryptographic key generation algorithm*]

[80] [*assignment: cryptographic key sizes*]

251 The Basic Terminal shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the Basic Terminal.

252 **FCS_COP.1/SHA_BT Cryptographic operation – Hash Function by the Basic Terminal**

Hierarchical to: No other components.

FCS_COP.1.1/ SHA_BT The **Basic Terminal** shall perform hashing[81] in accordance with a specified cryptographic algorithms SHA-1 [82] and cryptographic key sizes none [83] that meet the following: FIPS 180-2 [84].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

253 **Application note 59:** This SFR requires the terminal to implement the hash function SHA-1 for the cryptographic primitive to generate the Document Basic Access Keys according to FCS_CKM.1/KDF_BT.

254 **FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal**

Hierarchical to: No other components.

FCS_COP.1.1/ ENC_BT The **Basic Terminal** shall perform secure messaging – encryption and decryption[85] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[86] and cryptographic key sizes 112 bit[87] that meet the following: FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)[88].

[81] [assignment: *list of cryptographic operations*]

[82] [assignment: *cryptographic algorithm*]

[83] [assignment: *cryptographic key sizes*]

[84] [assignment: *list of standards*]

[85] [assignment: *list of cryptographic operations*]

[86] [assignment: *cryptographic algorithm*]

[87] [assignment: *cryptographic key sizes*]

[88] [assignment: *list of standards*]

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

255 **Application note 60:** This SFR requires the Basic Terminal to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The key is agreed between the TOE and the terminal during the execution of the Basic Access Control Authentication Mechanism. The key size of 112 bit is chosen to resist attacks with high attack potential.

256 **FCS_COP.1/MAC_BT Cryptographic operation – Secure messaging Message Authentication Code by the Basic Terminal**

Hierarchical to: No other components.

FCS_COP.1.1/ MAC_BT The **Basic Terminal** shall perform secure messaging – message authentication code[89] in accordance with a specified cryptographic algorithm Retail-MAC[90] and cryptographic key sizes 112 bit[91] that meet the following: FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2)[92].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

257 **Application note 61:** This SFR requires the terminal to implement the cryptographic primitive for secure messaging with message authentication code over the transmitted data. The key is agreed or defined as the key for secure messaging encryption. The key size of 112 bit is chosen to resist attacks with high attack potential.

258 The Basic Terminal shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (Common Criteria Part 2 extended).

259 **FCS_RND.1/BT Quality metric for random numbers - Basic Terminal**

Hierarchical to: No other components.

FCS_RND.1.1/BT The **Basic Terminal** shall provide a mechanism to generate random numbers that meets [assignment: *a defined quality metric*].

[89] [assignment: *list of cryptographic operations*]

[90] [assignment: *cryptographic algorithm*]

[91] [assignment: *cryptographic key sizes*]

[92] [assignment: *list of standards*]

Dependencies: No dependencies.

260 **Application note 62:** The ST writer shall perform the operation in FCS_RND.1.1/BT. This SFR requires the terminal to generate random numbers used in the authentication protocols as required by FCS_CKM.1/KDF_BT and FIA_UAU.4 The quality metric shall be chosen to ensure at least the strength of function Basic Access Control Authentication for the challenges.

261 The Basic Terminal shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

262 **FIA_UAU.4/BT Single-use authentication mechanisms – Basic Terminal**

Hierarchical to: No other components.

FIA_UAU.4.1/BT The **Basic Terminal** shall prevent reuse of authentication data related to Basic Access Control Authentication Mechanism [93].

Dependencies: No dependencies.

263 **Application note 63:** The Basic Access Control Authentication Mechanism [6] uses a challenge RND.IFD freshly and randomly generated by the terminal to prevent reuse of a response generated by a MRTD's chip and of the session keys from a successful run of authentication protocol.

264 The Basic Terminal shall meet the requirement "Re-authentication (FIA_UAU.6)" as specified below (Common Criteria Part 2).

265 **FIA_UAU.6/BT Re-authentication - Basic Terminal**

Hierarchical to: No other components.

FIA_UAU.6.1/BT The **Basic Terminal** shall re-authenticate the user under the conditions each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism [94].

Dependencies: No dependencies.

266 **Application note 64:** The Basic Access Control Mechanism specified in [6] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The terminal checks by secure messaging in MAC_ENC mode each MRTD's chip response to a command based on Retail-MAC whether it was sent by the successfully authenticated MRTD's chip. The authentication fails if any response is received with incorrect message authentication code.

[93] [assignment: *identified authentication mechanism(*s)]

[94] [assignment: *list of conditions under which re-authentication is required*]

5.3.4 General Inspection System

267 The General Inspection System (GIS) is a Basic Inspection System which implements additional the Chip Authentication Mechanism. Therefore it has to fulfil all security requirements of the Basic Inspection System as described above.

268 The General Inspection System verifies the authenticity of the MRTD's by the Chip Authentication Mechanism during inspection and establishes new secure messaging with keys. The reference data for the Chip Authentication Mechanism is the Chip Authentication Public Key read form the logical MRTD data group EF.DG14 and verified by Passive Authentication (cf. to FDP_DAU.1/DS). Note, that the Chip Authentication Mechanism requires the General Inspection System to verify at least one message authentication code of a response sent by the MRTD to check the authenticity of the chip.

269 The General Inspection System shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2).

270 **FCS_CKM.1/DH_GIS Cryptographic key generation – Diffie-Hellman Keys by the GIS**

Hierarchical to: No other components.

FCS_CKM.1.1/ DH_GIS The **General Inspection System** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [25], Annex A.1 [95].

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

271 **Application note 65:** The GIS generates a shared secret value with the terminal during the Chip Authentication Protocol, see [25], sec. 3.1 and Annex A.1. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. a modulo arithmetic based cryptographic algorithm, cf. [21]) or on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [25], Annex A.1, [26] and [20] for details). Even the General Inspection System shall support only the concrete algorithm implemented in the TOE it is expected that the General Inspection System will support both of them for interoperability reasons. The shared secret value is used to derive the 112 bit Triple-DES key for encryption and the 112 bit Retail-MAC keys according to the Document Basic Access Key Derivation Algorithm [6], annex E.1, for the TSF required by FCS_COP.1/ENC_MRTD and FCS_COP.1/MAC_MRTD.

272 **FCS_COP.1/SHA_GIS Cryptographic operation – Hash for Key Derivation by GIS**

Hierarchical to: No other components.

[95] [assignment: *list of standards*]

FCS_COP.1.1/ SHA_GIS The **General Inspection System** shall perform hashing[96] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes none[97] that meet the following: FIPS 180-2[98].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

273 **Application note 66:** The ST writer shall perform the missing operation for the assignment of the hash algorithm according to the hash function used by the TOE for Chip Authentication and therefore to be supported by the GIS. The Chip Authentication Protocol may use SHA-1 and SHA-256 (cf. [25], Annex A.1.3.3).

274 The General Inspection System shall meet the requirement “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (Common Criteria Part 2).

275 **FIA_UAU.4/GIS Single-use authentication mechanisms - Single-use authentication of the Terminal by the GIS**

Hierarchical to: No other components.

FIA_UAU.4.1/GIS The **General Inspection System** shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication Protocol[99].

Dependencies: No dependencies.

276 The General Inspection System shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below (Common Criteria Part 2).

277 **FIA_UAU.5/GIS Multiple authentication mechanisms – General Inspection System**

Hierarchical to: No other components.

FIA_UAU.5.1/GIS The **General Inspection System** shall provide

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication[100]

to support user authentication.

[96] [assignment: *list of cryptographic operations*]

[97] [assignment: *cryptographic key sizes*]

[98] [assignment: *list of standards*]

[99] [assignment: *identified authentication mechanism(*s)]

[100] [assignment: *list of multiple authentication mechanisms*]

FIA_UAU.5.2/GIS The **General Inspection System** shall authenticate any user's claimed identity according to the following rules:

1. The General Inspection System accepts the authentication attempt as MRTD only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
2. After successful authentication as MRTD and until the completion of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of secure messaging with key agreed with the authenticated MRTD by means of the Basic Access Control Authentication Mechanism.
3. After run of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.[101]

Dependencies: No dependencies.

278 **Application note 67:** Basic Access Control Mechanism includes the secure messaging for all commands and response codes exchanged after successful mutual authentication between the inspection system and the MRTD. The inspection system shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys drawn from the second, optical readable MZR line and the secure messaging after the mutual authentication. The General Inspection System and the MRTD shall use the secure messaging with the keys generated by the Chip Authentication Mechanism after the mutual authentication.

279 The General Inspection System shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2).

280 **FIA_UAU.6/GIS Re-authenticating – Re-authenticating of Terminal by the General Inspection System**

Hierarchical to: No other components.

[101] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

FIA_UAU.6.1/ GIS The **General Inspection System** shall re-authenticate the user under the conditions

1. Each response sent to the General Inspection System after successful authentication of the MRTD with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall have a correct MAC created by means of secure messaging keys agreed upon by the Basic Access Control Authentication Mechanism.
2. Each response sent to the General Inspection System after successful run of the Chip Authentication Protocol shall have a correct MAC created by means of secure messaging keys generated by Chip Authentication Protocol. [102]

Dependencies: No dependencies.

281 **Application note 68:** The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [6] include secure messaging for all commands and responses exchanged after successful authentication of the inspection system. The General Inspection System checks by secure messaging in MAC_ENC mode each response based on Retail-MAC whether it was sent by the successfully authenticated MRTD (see FCS_COP.1/MAC_MRTD for further details). The General Inspection System does not accept any response with incorrect message authentication code. Therefore the General Inspection System re-authenticate the user for each received command and accept only those responses received from the authenticated user.

282 The General Inspection System shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2).

283 **FDP_UCT.1/GIS Basic data exchange confidentiality - General Inspection System**

Hierarchical to: No other components.

FDP_UCT.1.1/GIS The **General Inspection System** shall enforce the Access Control SFP [103] to be able to transmit and receive[104] objects in a manner protected from unauthorised disclosure **after Chip Authentication**.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

284 The General Inspection System shall meet the requirement “Data exchange integrity (FDP_UIT.1)” as specified below (Common Criteria Part 2).

285 **FDP_UIT.1/GIS Data exchange integrity - General Inspection System**

Hierarchical to: No other components.

[102] [assignment: *list of conditions under which re-authentication is required*]

[103] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[104] [selection*: transmit, receive*]

FDP_UIT.1.1/GIS The **General Inspection System** shall enforce the Basic Access Control SFP [105] to be able to transmit and receive [106] user data in a manner protected from modification, deletion, insertion and replay [107] errors **after Chip Authentication**.

FDP_UIT.1.2/GIS The **General Inspection System** shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [108] has occurred **after Chip Authentication**.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

5.3.5 Extended Inspection System

286 The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

287 **FCS_COP.1/SIG_SIGN_EIS Cryptographic operation – Signature creation by EIS**

Hierarchical to: No other components.

FCS_COP.1.1/SIG_SIGN_EIS The **Extended Inspection System** shall perform signature creation [109] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

288 **Application note 69:** The ST writer shall perform the missing operation of the assignments for the signature algorithms key lengths and standards to be implemented by the Extended Inspection system for the Terminal Authentication Protocol compliant with the TOE (cf. [25], Annex A.2.1.1 and C.3 for details).

289 **FCS_COP.1/SHA_EIS Cryptographic operation – Hash for Key Derivation by EIS**

Hierarchical to: No other components.

[105] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[106] [selection*: transmit, receive*]

[107] [selection: *modification, deletion, insertion, replay*]

[108] [selection: *modification, deletion, insertion, replay*]

[109] [assignment: *list of cryptographic operations*]

FCS_COP.1.1/ SHA_EIS The **Extended Inspection System** shall perform hashing [110] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes none [111] that meet the following: FIPS 180-2 [112].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

290 **Application note 70:** The ST writer shall perform the missing operation for the assignment of the hash algorithm supported by the TOE. The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism (cf. [6], annex E.1). The TOE may implement additional hash functions SHA-224, SHA-256, SHA-384 and SHA-512 for the Terminal Authentication Protocol (cf. [25], Annex A.2.1.1 and C.3 for details).

291 The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended).

292 **FIA_API.1/EIS Authentication Proof of Identity – Extended Inspection System**

Hierarchical to: No other components.

FIA_API.1.1/EIS The **Extended Inspection System** shall provide a Terminal Authentication Protocol according to [25] [113] to prove the identity of the Extended Inspection system [114].

Dependencies: No dependencies.

293 **Application note 71:** This SFR requires the Extended Inspection system to implement the Terminal Authentication Mechanism specified in [25], sec. 3.3. The Extended Inspection system requests a challenge of 8 Byte from the MRTD and generates a digital signature using RSA or ECDSA (cf. [25], appendix A.2.1 for details).

5.3.6 Personalization Terminals

294 The TOE supports different authentication and access control mechanisms which may be used for the Personalization Agent depending on the personalization scheme of the Issuing State or Organization:

(1) The Basic Access Control Mechanism which may be used by the Personalization Terminal with a Personalization Agent Secret Key Pair. The Basic Access Control Mechanism

[110] [assignment: *list of cryptographic operations*]

[111] [assignment: *cryptographic key sizes*]

[112] [assignment: *list of standards*]

[113] [assignment: *authentication mechanism*]

[114] [assignment: *authorized user or rule*]

establishes strong cryptographic keys for the secure messaging to ensure the confidentiality by Triple-DES and integrity by Retail-MAC of the transmitted data. This approach may be used in a personalization environment where the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.

(2) The Personalization Terminal may use the Terminal Authentication Protocol like a Extended Inspection System but using the Personalization Agent Keys to authenticate themselves to the TOE. This approach may be used in a personalization environment where (i) the Personalization Agent want to authenticate the MRTD's chip and (ii) the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.

(3) In a centralized personalization scheme the major issue is high productivity of personalization in a high secure environment. In this case the personalization agent may wish to reduce the protocol to symmetric authentication of the terminal without secure messaging. Therefore the TOE and the Personalization Terminal support a simple the Symmetric Authentication Mechanism with Personalization Agent Key as requested by the SFR FIA_UAU.4/MRTD and FIA_API.1/SYM_PT.

295 The Personalization Terminal shall meet the requirement "Authentication Prove of Identity (FIA_API)" as specified below (Common Criteria Part 2 extended) if it uses the Symmetric Authentication Mechanism with Personalization Agent Key.

296 **FIA_API.1/SYM_PT Authentication Proof of Identity - Personalization Terminal Authentication with Symmetric Key**

Hierarchical to: No other components.

FIA_API.1.1/ SYM_PT	The **Personalization Terminal** shall provide an Authentication Mechanism based on Triple-DES **[115]** to prove the identity of the Personalization Agent **[116]**.

Dependencies: No dependencies.

297 **Application note 72:** The Symmetric Authentication Mechanism for Personalization Agents is intended to be used in a high secure personalization environment only. It uses the symmetric cryptographic Personalization Agent Authentication Secret key of 112 bits to encrypt a challenge of 8 Bytes with Triple-DES which the terminal receives from the MRTD's chip e.g. as response of a GET CHALLENGE. The answer may be sent by means of the EXTERNAL AUTHENTICATE command according to ISO 7816-4 [27] command. In this case the communication may be performed without secure messaging (note, that FIA_UAU.5.2 requires secure messaging only after run of Basic Access Control Authentication).

[115] [assignment: *authentication mechanism*]

[116] [assignment: *authorized user or rule*]

6 PP Application Notes

298 There are no sensitive application notes for the protection profile.

7 Rationales

7.1 Security Objectives Rationale

299 The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OD.Assurance	OD.Material	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System
T.Chip-ID				x	x														x	
T.Skimming			x																	
T.Read_Sensitive_Data				x												x				x
T.Forgery	x	x							x					x			x	x		
T.Counterfeit						x						x			x		x			
T.Abuse-Func							x													
T.Information_Leakage								x												
T.Phys-tamper									x											
T.Malfunction										x										
P.Manufact											x	x								
P.Personalization	x										x		x							
P.Personal_Data		x	x																x	
P.Sensitive_Data				x												x				x
A.Pers_Agent													x							
A.Insp_Sys																	x		x	
A.Signature_PKI														x			x			
A.Auth_PKI																x				x

Table 2: Security Objective Rationale

300 The OSP **P.Manufact** “Manufacturing of the MRTD’s chip” requires the quality and integrity of the manufacturing process and control the MRTD’s material in the Phase 2 Manufacturing including unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data. The security objective for the TOE environment **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment” address these obligations of the IC Manufacturer and MRTD Manufacturer. **OD.Material** “Control over MRTD material” ensures that materials, equipment and tools used to produce genuine and

authentic MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs.

301 The OSP **P.Personalization** "Personalization of the MRTD by issuing State or Organization only" addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD", and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD". Note, the manufacturer equips the TOE with the Personalization Agent Authentication key(s) according to **OD.Assurance** "Assurance Security Measures in Development and Manufacturing Environment". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalization Agent.

302 The OSP **P.Personal_Data** "Personal data protection policy" requires that the logical MRTD can be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an inspection system. This OSP is covered by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the secure messaging based on session keys agreed in this protocol. The security objective **OT.Data_Conf** requires the TOE to implement the Basic Access Control as defined by ICAO [6] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The security objective **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" requires the inspection system to protect their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. After successful Chip Authentication the security objective **OT.Data_Conf** "Confidentiality of personal data" ensures the confidentiality of the logical MRTD data during their transmission to the General Inspection System.

303 The OSP **P.Sensitive_Data** "Privacy of sensitive biometric reference data" is fulfilled and the threat **T.Read_Sensitive_Data** "Read the sensitive biometric reference data" is countered by the TOE-objective **OT.Sens_Data_Conf** "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorised inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorisation bases on Document Verifier certificates issued by the issuing state or organisation as required by **OE.Authoriz_Sens_Data** "Authorisation for use of sensitive biometric reference data". The Document Verifier of the receiving state has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** "Authorisation of Extended Inspection Systems".

304 The threat **T.Chip_ID** "Identification of MRTD's chip" addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the contactless communication interface. This threat is countered by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the secure messaging based on session keys agreed in this protocol. The security objective **OT.Identification** "Identification and Authentication of the TOE" by limiting the TOE chip identification to the Basic Inspection System. The security objective **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" requires the inspection system to protect to their communication (as Basic Inspection System) with the TOE before secure messaging based on the Chip Authentication Protocol is successfully established. After successful Chip Authentication the security objective OT.Data_Conf "Confidentiality of personal data" ensures the confidentiality of the logical MRTD data during their transmission to the General Inspection System.

305 The threat **T.Skimming** "Skimming digital MRZ data or the digital portrait" addresses the reading of the logical MRTD trough the contactless interface outside the communication between the MRTD's chip and Inspection System. This threat is countered by the security objective **OT.Data_Conf** "Confidentiality of personal data" through Basic Access Control allowing read data access only after successful authentication of the Basic Inspection System.

306 The threat **T.Forgery** "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The examination of the presented MRTD passport book according to **OE.Exam_MRTD** "Examination of the MRTD passport book" shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign "**Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Passive_Auth_Verif** "Verification by Passive Authentication".

307 The threat **T.Counterfeit** "MRTD's chip" addresses the attack of unauthorised copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of MRTD's chip authentication" using a authentication key pair to be generated by the issuing state or organisation. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_MRTD** "MRTD Authentication Key". According to **OE.Exam_MRTD** "Examination of the MRTD passport book" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip. MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs targeted on by **OD.Material**.

308 The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks of misusing MRTD's functionality to disable or bypass the TSFs. The security objective for the TOE **OT.Prot_Abuse-Func** "Protection against abuse of functionality" ensures that the usage of functions which may not be used in the operational phase is effectively prevented. Therefore attacks intending to abuse functionality in order to disclose or manipulate critical (User) Data or to affect the TOE in such a way that security features or TOE's functions may be bypassed, deactivated, changed or explored shall be effectively countered.

309 The threats **T.Information_Leakage** "Information Leakage from MRTD's chip", **T.Phys-Tamper** "Physical Tampering" and **T.Malfunction** "Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot_Inf_Leak** "Protection against Information Leakage", **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" and **OT.Prot_Malfunction** "Protection against Malfunctions".

310 The assumption **A.Pers_Agent** "Personalization of the MRTD's chip" is covered by the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD" including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data and the enabling of security features of the TOE according to the decision of the Issuing State or Organization concerning the Basic Access Control.

311 The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** “Inspection Systems for global interoperability” is covered by the security objectives for the TOE environment **OE.Exam_MRTD** “Examination of the MRTD passport book” which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD’s chip. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD” requirethe Inspection System to protect the logical MRTD data during the transmission and the internal handling.

312 The assumption **A.Signature_PKI** “PKI for Passive Authentication” is directly covered by the security objective for the TOE environment **OE.Pass_Auth_Sign “**Authentication of logical MRTD by Signature” covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_MRTD** “Examination of the MRTD passport book”.

313 The assumption **A.Auth_PKI** “PKI for Inspection Systems” is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** “Authorisation for use of sensitive biometric reference data” requires the CVCA to limit the read access to sensitive biometric by issuing Document Verifier certificates for authorised receiving States or Organisations only. The Document Verifier of the receiving state is required by **OE.Ext_Insp_Systems** “Authorisation of Extended Inspection Systems” to authorise Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organisation has to establish the necessary public key infrastructure.

7.2 Security Requirements Rationale

7.2.1 Security Functional Requirements Rationale

314 The following table provides an overview for security functional requirements coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion
FAU_SAS.1					x					
FCS_CKM.1/KDF_MRTD	x	x	x	x		x				
FCS_CKM.1/DH_MRTD	x	x		x		x				
FCS_CKM.4/MRTD	x	x	x	x						
FCS_COP.1/SHA_MRTD	x	x	x	x		x				
FCS_COP.1/TDES_MRTD	x	x	x			x				
FCS_COP.1/MAC_MRTD	x	x	x	x		x				

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion
FCS_COP.1/SIG_VER	x			x						
FCS_RND.1/MRTD	x			x						
FIA_UID.1	x	x	x	x	x					
FIA_UAU.1	x	x	x	x	x					
FIA_UAU.4/MRTD	x	x	x	x						
FIA_UAU.5/MRTD	x	x	x	x						
FIA_UAU.6/MRTD	x	x	x	x						
FIA_AFL.1			x							
FIA_API.1/CAP						x				
FDP_ACC.1	x	x	x	x						
FDP_ACF.1	x	x	x	x						
FDP_UCT.1/MRTD			x	x						
FDP_UIT.1/MRTD		x		x						
FMT_SMF.1	x	x	x							
FMT_SMR.1	x	x	x							
FMT_LIM.1							x			
FMT_LIM.2							x			
FMT_MTD.1/INI_ENA					x					
FMT_MTD.1/INI_DIS					x					
FMT_MTD.1/CVCA_INI				x						
FMT_MTD.1/CVCA_UPD				x						
FMT_MTD.1/DATE				x						
FMT_MTD.1/KEY_WRITE	x		x							
FMT_MTD.1/CAPK		x	x	x		x				
FMT_MTD.1/KEY_READ	x	x	x	x		x				
FMT_MTD.3				x						
FPT_EMSEC.1	x							x		
FPT_TST.1								x		x
FPT_RVM.1							x			
FPT_FLS.1								x		x
FPT_PHP.3								x	x	
FPT_SEP.1							x			x

Table 3: Coverage of Security Objective for the TOE by SFR

315 The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" addresses the access control of the writing the logical MRTD and the management of the TSF for Basic Access Control. The write access to the logical MRTD data are defined by the SFR FIA_UID.1, FIA_UAU.1, FDP_ACC.1 and FDP_ACF.1 in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Control.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD and FIA_UAU.5/MRTD. If the Basic Access Control Authentication Mechanism with the Personalization Agent Authentication Key is used the TOE will use the FCS_RND.1/MRTD (for the generation of the challenge), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the session keys), FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode secure messaging) and FIA_UAU.6/MRTD (for the re-authentication). If the Personalization Terminal want to authenticate themselves to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1/MRTD (for the generation of the challenge), FCS_CKM.1/DH_MRTD, FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6/MRTD (for the re-authentication). If the Personalization Terminal wants to authenticate themselves to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1/MRTD (for the generation of the challenge) and FCS_COP.1/TDES_MRTD (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMSEC.1 the confidentially of these keys.

316 The security objective **OT.Data_Int** "Integrity of personal data" requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1 and FIA_UAU.1 before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

The TOE supports the inspection system detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD. The SFR FIA_UAU.6/MRTD and FDP_UIT.1/MRTD requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/DH_MRTD (for the generation of shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and

FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

317 The security objective **OT.Data_Conf** "Confidentiality of personal data" requires the TOE to ensure the confidentiality of the logical MRTD data in EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: only the successful authenticated Personalization Agent, Basic Inspection Systems[117] and Extended Inspection Systems are allowed to read the data of the logical MRTD. The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys). The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

The SFR FIA_AFL.1 strengthens the authentication function as terminal part of the Basic Access Control Authentication Protocol or other authentication functions if necessary. The SFR FIA_UAU.4/MRTD prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5/MRTD enforces the TOE (i) to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and (ii) to accept chip authentication only after successful authentication as Basic Inspection System. Moreover, the SFR FIA_UAU.6/MRTD requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

After Chip authentication the TOE and the General Inspection System establish protection of the communication by secure messaging (cf. the SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD) in ENC_MAC_Mode by means of the cryptographic functions according to FCS_CKM.1/DH_MRTD (for the generation of shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5/MRTD requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

318 The security objective **OT.Sense_Data_Conf** "Confidentiality of sensitive biometric reference data" is enforced by the Access Control SFP defined in FDP_ACC.1 and FDP_ACF.1 allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorised by a validly verifiable certificate according FCS_COP.1/SIG_VER.

The SFR FIA_UID.1 and FIA_UAU.1 requires authentication of the inspection systems. The SFR FIA_UAU.5/MRTD requires the successful Chip Authentication before any authentication

[117] Note the General Inspection Systems use the role Basic Inspection System.

attempt as Extended Inspection System. The SFR FIA_UAU.6/MRTD and FDP_UCT.1/MRTD requires the confidentiality protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1/MRTD (for the generation of the terminal authentication challenge), FCS_CKM.1/DH_MRTD (for the generation of shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA's public key and certificate as well as the current date are written or update by authorised identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

319 The security objective **OT.Identification** "Identification and Authentication of the TOE" address the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

The TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 "Operational Use". The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data. The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their use in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. Application note 32).

320 The security objective **OT.Chip_Auth_Proof** "Proof of MRTD's chip authenticity" is ensured by the Chip Authentication Protocol provided by FIA_API.1/CAP proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1/DH_MRTD is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol [25] requires additional TSF according to FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the session keys), FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode secure messaging).

321 The security objective **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality" is ensured by (i) the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other which may not be used after TOE Delivery, (ii) the SFR FPT_RVM.1 which prevents by monitoring the bypass and deactivation of security features or functions of the TOE, and (iii) the SFR FPT_SEP.1 which prevents change or explore security features or functions of the TOE by means of separation the other TOE functions.

322 The security objective **OT.Prot_Inf_Leak** "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the MRTD's chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMSEC.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or

- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

323 The security objective **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" is covered by the SFR FPT_PHP.3.

324 The security objective **OT.Prot_Malfunction** "Protection against Malfunctions" is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction, and (iii) the SFR FPT_SEP.1 limiting the effects of malfunctions due to TSF domain separation.

325 The security objectives **OD.Assurance** and **OD.Material** for the IT environment will be supported by non-IT security measures only.

326 The security objective **OE.Authoriz_Sens_Data** is directed to establish the Document Verifier PKI and will be supported by non-IT security measures only.

327 The following table provides an overview how security functional requirements for the IT environment cover security objectives for the TOE environment. The protection profile describes only those SFR of the IT environment directly related to the SFR for the TOE.

	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System
Document Signer								
FDP_DAU.1/DS		x	x		x	x		
Document Verification PKI								
FCS_CKM.1/PKI				x				
FCS_COP.1/CERT_SIGN				x				
Basic Inspection System								
FCS_CKM.1/KDF_BT	x				x		x	
FCS_CKM.4/BT					x		x	
FCS_COP.1/SHA_BT	x				x		x	
FCS_COP.1/ENC_BT	x				x		x	
FCS_COP.1/MAC_BT	x				x		x	
FCS_RND.1/BT	x				x		x	
FIA_UAU.4/BT	x				x		x	
FIA_UAU.6/BT	x				x		x	
General Inspection System								

	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System
FCS_CKM.1/DH_GIS	x				x			
FCS_COP.1/SHA_GIS	x				x			
FIA_UAU.4/GIS					x			
FIA_UAU.5/GIS					x		x	
FIA_UAU.6/GIS					x		x	
FDP_UCT.1/GIS	x				x		x	
FDP_UIT.1/GIS	x				x		x	
Extended Inspection System								
FCS_COP.1/SIG_SIGN_EIS	x							x
FCS_COP.1/SHA_EIS	x							x
FIA_API.1/EIS	x							x
Personalization Agent								
FIA_API.1/SYM_PT	x							

Table 4: Coverage of Security Objectives for the IT environment by SFR

328 The **OE.Personalization** “Personalization of logical MRTD” requires the Personalization Terminal to authenticate themselves to the MRTD’s chip to get the write authorization.

If the Basic Access Control Authentication Mechanism with the Personalization Agent Authentication Key is used the Personalization Terminal will use the FCS_RND.1/BT (for the generation of the challenge), FCS_CKM.1/KDF_BT, FCS_COP.1/SHA_BT (for the derivation of the session keys), and FCS_COP.1/ENC_BT and FCS_COP.1/MAC_BT (for the ENC_MAC_Mode secure messaging) to authenticate themselves and to protect the personalization data during transfer.

If the Personalization Terminal want to authenticate themselves to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the Personalization Terminal will use TSF according to the FCS_RND.1/BT (for the generation of the challenge), FCS_CKM.1/DH_GIS, FCS_CKM.1/KDF_BT, FCS_COP.1/SHA_GIS (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_SIGN_EIS, FCS_COP.1/SHA_EIS and FIA_API.1/EIS (as part of the Terminal Authentication Protocol).

If the Personalization Terminal wants to authenticate themselves to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the SFR FIA_API.1/SYM_PT, FCS_RND.1/MRTD (for the generation of the challenge) and FCS_COP.1/TDES_MRTD (to verify the authentication attempt). Using the keys derived by means of the Chip Authentication Mechanism the Personalisation Agent will transfer MRTD holder's personalisation data (identity, biographic data, correctly enrolled biometric reference data) in a confidential and integrity protected manner as required by FDP_UCT.1/GIS and FDP_UIT.1/GIS.

329 The **OE.Pass_Auth_Sign** "Authentication of logical MRTD Signature" is covered by FDP_DAU.1/DS which requires the Document Signer to provide a capability to generate evidence for the validity of EF.DG1 to EF.DG16 and the Document Security Objects and therefore, to support the inspection system to verify the logical MRTD.

330 The **OE.Auth_Key_MRTD** "MRTD Authentication Key" is covered by FDP_DAU.1/DS which requires the Document Signer to provide a capability to generate evidence for the validity of chip authentication public key in DG 14. There is no need for the PP to provide any specific requirement for the method of generation, distribution and handling of the Chip Authentication Private Key by the IT environment.

331 The **OE.Authoriz_Sens_Data** "Authorization for Use of Sensitive Biometric Reference Data" addresses the establishment of the Document Verification PKI which include cryptographic key generation for the Document Verification PKI Keys and the signing of the certificates. The SFR FCS_CKM.1/PKI and FCS_COP.1/CERT_SIGN enforce that these cryptographic functions fit the signature verification function for the certificates and the terminal authentication addressed by FCS_COP.1/SIG_VER.

332 The **OE.Exam_MRTD** "Examination of the MRTD passport book" requires the Basic Inspection System for global interoperability to implement the terminal part of the Basic Access Control [6] as required by FCS_CKM.1/KDF_BT, FCS_CKM.4/BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT, FCS_RND.1/BT, FIA_UAU.4/BT and FIA_UAU.6/BT. The verification of the authenticity of the MRTD's chip by General Inspection Systems and Extended Inspection Systems (including the functionality of the GIS) is covered by the FCS_CKM.1/DH_GIS, FCS_COP.1/SHA_GIS, FIA_UAU.4/GIS, FIA_UAU.5/GIS and FIA_UAU.6/GIS providing the Chip Authentication Protocol and checking continuously the messages received from the MRTD's chip. The authenticity of the Chip Authentication Public Key (EF.DG14) is ensured by FDP_DAU.1/DS.

333 The **OE.Pass_Auth_Verif** "Verification by Passive Authentication" is covered by the SFR FDP_DAU.1/DS.

334 The security objective **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" addresses the protection of the logical MRTD during the transmission and internal handling. The SFR FIA_UAU.4/BT, FIA_UAU.5/GIS and FIA_UAU.6/BT address the terminal part of the Basic Access Control Authentication Mechanism and FDP_UCT.1/GIS and FDP_UIT.1/BT the secure messaging established by the Chip Authentication mechanism. The SFR FCS_CKM.1/KDF_BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT and FCS_RND.1/BT as well as FCS_CKM.4/BT are necessary to implement this mechanism. The BIS shall destroy the Document Access Control Key and the secure messaging keys after inspection of the MRTD according to FCS_CKM.4 because they are not needed any more.

335 .The **OE.Ext_Insp_System** "Authorisation of Extended Inspection Systems" is covered by the Terminal Authentication Protocol proving the identity of the EIS as required by FIA_API.1/EIS basing on signature creation as required by FCS_COP.1/SIG_SIGN_EIS and including a hash calculation according FCS_COP.1/SHA_EIS.

7.2.2 Dependency Rationale

336 The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

337 The table 5 shows the dependencies between the SFR and of the SFR to the SAR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1/KDF_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD justification 1 for non-satisfied dependencies
FCS_CKM.1/DH_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD justification 2 for non-satisfied dependencies
FCS_CKM.4/MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes	FCS_CKM.1, justification 1 for non-satisfied dependencies
FCS_COP.1/SHA_MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 3 for non-satisfied dependencies
FCS_COP.1/TDES_MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 4 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/MAC_MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 4 for non-satisfied dependencies
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 5 for non-satisfied dependencies
FCS_RND.1/MRTD	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UAU.1 Timing of authentication	Fulfilled
FIA_UAU.4/MRTD	No dependencies	n.a.
FIA_UAU.5/MRTD	No dependencies	n.a.
FIA_UAU.6/MRTD	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled
FIA_API.1/CAP	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.1, justification 6 for non-satisfied dependencies
FDP_UCT.1/MRTD	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1 justification 7 for non-satisfied dependencies
FDP_UIT.1/MRTD	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1, justification 7 for non-satisfied dependencies
FMT_SMF.1	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled
FMT_LIM.1	FMT_LIM.2	Fulfilled
FMT_LIM.2	FMT_LIM.1	Fulfilled
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.3	ADV_SPM.1, FMT_MTD.1	fulfilled
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	ADV_SPM.1	Fulfilled by EAL4
FPT_PHP.3	No dependencies	n.a.
FPT_RVM.1	No dependencies	n.a.
FPT_SEP.1	No dependencies	n.a.
FPT_TST.1	FPT_AMT.1 Abstract machine testing	See justification 8 for non-satisfied dependencies

Table 5: Dependencies between the SFR for the TOE

338 Justification for non-satisfied dependencies between the SFR for TOE:

No. 1: The SFR FCS_CKM.1/KDF_MRTD uses only the Document Basic Access Keys or other shared secrets to generate the secure messaging keys used for FCS_COP.1/TDES and FCS_COP.1/MAC. The SFR FCS_CKM.4/MRTD destroys these keys automatically. These simple processes do not need any special security attributes for the secure messaging keys.

No. 2: The SFR FCS_CKM.1/DH_MRTD calculates shared secrets to generate the secure messaging keys used for FCS_COP.1/TDES and FCS_COP.1/MAC. The SFR FCS_CKM.4/MRTD destroys these keys automatically. These simple processes do not need any special security attributes for the secure messaging keys.

No. 3: The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFRs are needed to be defined for this specific instantiation of FCS_COP.1.

No. 4: The SFR FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD use the automatically generated secure messaging keys assigned to the session with the successfully authenticated BIS only. There is no need for any special security attributes for the secure messaging keys.

No. 5: The SFR FCS_COP.1/SIG_VER uses the initial public key Country Verifying Certification Authority and the public keys in certificates provided by the terminals as TSF data for the Terminal Authentication Protocol and the Access Control. Their validity verified according to FMT_MDT.3 and their security attributes are managed by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. There is no need to import user data or manage their security attributes.

No. 6: The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.2) is necessary here.

No. 7: The SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the use secure messaging between the MRTD and the BIS. There is no need for sensitive SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels it is the only one.

No. 8: The TOE consists of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

339 The following table shows the dependencies between the SFR for the IT environment and of the SFR to the SAR of the TOE.

SFR	Dependencies	Support of the Dependencies
FDP_DAU.1	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/PKI	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 9 for non-satisfied dependencies
FCS_COP.1/CERT_SIGN	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 9 for non-satisfied dependencies
FCS_CKM.1/KDF_BT	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1/TDES_BT, FCS_COP.1/MAC_BT justification 10 for non-satisfied dependencies
FCS_CKM.4/BT	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes	FCS_CKM.1, justification 10 for non-satisfied dependencies
FCS_COP.1/SHA_BT	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 11 for non-satisfied dependencies
FCS_COP.1/ENC_BT	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 12 for non-satisfied dependencies
FCS_COP.1/MAC_BT	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with	FCS_CKM.1, FCS_CKM.4, justification 12 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	
FCS_RND.1/BT	No dependencies	n.a.
FIA_UAU.4/BT	No dependencies	n.a.
FIA_UAU.6/BT	No dependencies	n.a.
FCS_CKM.1/DH_GIS	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_COP.1/MAC_BT, FCS_CKM.4/BT, justification 13 for non-satisfied dependencies
FCS_COP.1/SHA_GIS	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_COP.1/MAC_BT, FCS_CKM.4/BT, justification 13 for non-satisfied dependencies
FIA_UAU.4/GIS	No dependencies	n.a.
FIA_UAU.5/GIS	No dependencies	n.a.
FIA_UAU.6/GIS	No dependencies	n.a.
FDP_UCT.1/GIS	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	justification 14 for non-satisfied dependencies
FDP_UIT.1/GIS	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	justification 14 for non-satisfied dependencies
FCS_COP.1/SIG_SIGN_EIS	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 15 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/SHA_EIS	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 15 for non-satisfied dependencies
FIA_API.1/EIS	No dependencies	n.a.
FIA_API.1/SYM_PT	No dependencies	n.a.

Table 6: Dependencies between the SFR for the IT environment

340 Justification for non-satisfied dependencies between the SFR for the IT environment.

No. 9: The TOE does not have specific functional security requirements to the IT environment establishing Document Verification PKI which have to be described by the listed dependency here.

No. 10: The SFR FCS_CKM.1/KDF_BT derives the Document Basic Access Keys and uses this key to generate the secure messaging keys used for FCS_COP.1/TDES and FCS_COP.1/MAC. The SFR FCS_CKM.4/BT destroys these keys. These processes do not need any special security attributes for the secure messaging keys.

No. 11: The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFR is needed to be defined for this specific instantiation of FCS_COP.1.

No. 12: The SFR FCS_COP.1/TDES_BT and FCS_COP.1/MAC_BT use the automatically generated secure messaging keys assigned to the session with the successfully authenticated MRTD only. There is no need for any special security attributes for the secure messaging keys.

No. 13: The SFR FCS_CKM.1/DH_GIS and FCS_COP.1/SHA_GIS are used for generation of secure messaging session keys (cf. FCS_COP.1/SHA_GIS, application note 66) by means of the Chip Authentication Protocol. These session keys are destroyed by the same function as for the Basic Terminal (cf. FCS_CKM.4/BT). There is no need for import or management of security attributes of these session keys.

No. 14: The SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the use secure messaging between the MRTD and the GIS as described by the FDP_UCT.1/GIS and FDP_UIT.1/GIS. There is no need to provide further description of this communication.

No. 15: The SFR FCS_COP.1/SIGN_EIS and FCS_COP.1/SHA_EIS are used by the Extended Inspection System for the proof of identity to the TOE by means of the Terminal Authentication Key Pair. The TOE does not have any specific requirements for the method of importing (cf. FDP_ITC.1 or FDP_ITC.2) or generation (cf. FCS_CKM.1) of the Terminal Authentication Key Pair, which is completely up to the IT environment.

7.2.3 Security Assurance Requirements Rationale

341 The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

342 The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the MRTD’s chip especially for the absence of unintended functionality.

343 The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD’s development and manufacturing especially for the secure handling of the MRTD’s material.

344 The selection of the component AVA_MSU.3 provides a higher assurance of the security of the MRTD’s usage especially in phase 3 “Personalization of the MRTD” and Phase 4 “Operational Use”. It is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

345 The minimal strength of function “high” was selected to ensure resistance against direct attacks on functions based on probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE to fulfil the OT.Sens_Data_Conf and OT.Chip_Auth_Proof. This is consistent with the security objective OD.Assurance.

346 The selection of the component AVA_VLA.4 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives OT.Sens_Data_Conf, OT.Chip_Auth_Proof and OD.Assurance.

347 The component ADV_IMP.2 has the following dependencies:

- ADV_LLD.1 Descriptive low-level design
- ADV_RCR.1 Informal correspondence demonstration
- ALC_TAT.1 Well-defined development tools

All of these are met or exceeded in the EAL4 assurance package.

348 The component ALC_DVS.2 has no dependencies.

349 The component AVA_MSU.3 has the following dependencies:

- ADO_IGS.1 Installation, generation, and start-up procedures
- ADV_FSP.1 Informal functional specification
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

350 The component AVA_VLA.4 has the following dependencies:

- ADV_FSP.1 Informal functional specification
- ADV_HLD.2 Security enforcing high-level design
- ADV_IMP.1 Subset of the implementation of the TSF

- ADV_LLD.1 Descriptive low-level design
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.

7.2.4 Security Requirements – Mutual Support and Internal Consistency

351 The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

352 The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis in section 7.2.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 7.2.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

353 Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 7.2.2 Dependency Rationale and 7.2.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 7.2.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

8 Glossary and Acronyms

Term	Definition
Active Authentication	Security mechanism defined in [6] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [6] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys. drawn form printed MRZ data for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [7]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [7]
Country Signing CA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing Country or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD. It is
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying

Term	Definition
	Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [6], Annex E.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [6]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (C_{DS}). [6]
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations
Eavesdropper	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [8]
Extended Access Control	Security mechanism identified in [6] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [7]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from

Term	Definition
	systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [8]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person’s document. [7]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else’s travel document or visa; or (d) no travel document or visa, if required. [8]
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD’s material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveller (the MRTD holder) and verifying its authenticity. [8]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD’s chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD’s chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [5]
Issuing State	The Country issuing the MRTD. [5]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [5]. The capacity expansion technology used is the MRTD’s chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [5] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16).
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to)

Term	Definition
	(1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [5]
Machine readable visa (MRV):	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [5]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [5]
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [7]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [5], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13 and EF.DG16) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO, [9], p. 14.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the portrait, signature and biographical data are applied

Term	Definition
	to the document. [7]
Personalization Agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/SYM_PT and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.
Receiving State	The Country to which the MRTD holder is applying for entry. [5]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [7]
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be all valid for the Current Date.
Travel document	A passport or other official document of identity issued by a State or organization which may be used by the rightful holder for international travel. [8]

Term	Definition
Traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalized MRTD	MRTD material prepared to produce a personalized MRTD containing an initialised and pre-personalized MRTD's chip.
User data	Data created by and for the user that does not affect the operation of the TSF (CC part 1 [1]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. [8]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
BIS	Basic Inspection System
CC	Common Criteria
EIS	Extended Inspection System
n.a.	Not applicable
OSP	Organisational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
TOE	Target of Evaluation
TSF	TOE security functions

9 Literature

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-08-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-08-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-08-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

ICAO

[5] Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18

[6] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

[7] ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

[8] BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 1.9, ICAO TAG MRTD/NTWG, 19 May 2003

[9] INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

[10] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version – 0.42 - Draft, August, 2004, Dr. Kügler, BSI

Cryptography

[11] Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, Bonn, 10.8.2004 (Zieldatum der Veröffentlichung ist Januar 2005)

[12] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[13] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[14] Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[15] Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[16] AMERICAN NATIONAL STANDARD X9.62-1999: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©, September 20, 1998

[17] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002

[18] ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002.

[19] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.

[20] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[21] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

Protection Profiles

[22] PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[23] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

[24] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-PP-0017, 18 August 2005

Other

[25] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.0, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI),

[26] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.

[27] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004